



# UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE  
United States Patent and Trademark Office  
Address: COMMISSIONER FOR PATENTS  
P.O. Box 1450  
Alexandria, Virginia 22313-1450  
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/844,448	04/27/2001	Gregory Neil Houston	05456.105005	9082

7590

04/20/2006

W. Scott Petty, Esq.  
KING & SPALDING  
45th Floor  
191 Peachtree Street, N.E.  
Atlanta, GA 30303

EXAMINER
----------

SON, LINH L D

ART UNIT	PAPER NUMBER
----------	--------------

2135

DATE MAILED: 04/20/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

**Office Action Summary**

Application No.

09/844,448

Applicant(s)

HOUSTON ET AL.

Examiner

Linh LD Son

Art Unit

2135

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

**Period for Reply**

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

**Status**

- 1) ☒ Responsive to communication(s) filed on 14 September 2005.
- 2a) ☐ This action is **FINAL**. 2b) ☒ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

**Disposition of Claims**

- 4) ☒ Claim(s) 1-59 is/are pending in the application.
- 4a) Of the above claim(s) \_\_\_\_\_ is/are withdrawn from consideration.
- 5) ☐ Claim(s) \_\_\_\_\_ is/are allowed.
- 6) ☒ Claim(s) 1-59 is/are rejected.
- 7) ☐ Claim(s) \_\_\_\_\_ is/are objected to.
- 8) ☐ Claim(s) \_\_\_\_\_ are subject to restriction and/or election requirement.

**Application Papers**

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☐ The drawing(s) filed on \_\_\_\_\_ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.  
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).  
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

**Priority under 35 U.S.C. § 119**

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some \* c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
  2. ☐ Certified copies of the priority documents have been received in Application No. \_\_\_\_\_.
  3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

\* See the attached detailed Office action for a list of the certified copies not received.

**Attachment(s)**

- |   |   |
|---|---|
| 1) <input type="checkbox"/> Notice of References Cited (PTO-892)  | 4) <input type="checkbox"/> Interview Summary (PTO-413)<br>Paper No(s)/Mail Date. _____ |
| 2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948)  | 5) <input type="checkbox"/> Notice of Informal Patent Application (PTO-152)             |
| 3) <input checked="" type="checkbox"/> Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)<br>Paper No(s)/Mail Date <u>09/05 (49 pgs)</u> . | 6) <input type="checkbox"/> Other: _____  |

**DETAILED ACTION**

1. This Office Action is responding to the RCE received on 09/14/05.
2. Claims 1, 16, 27, 34, 49 are amended.
3. Claims 1-59 are pending.

***Claim Rejections - 35 USC § 102***

4. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

Art Unit: 2135

5. Claims 1-11, 13-22, 24-44, 46-55, and 57-59 are rejected under 35 U.S.C. 102(e) as being anticipated by Hill et al, US Patent No. 6088804, hereinafter "Hill" (Cited in PTO 892 01/22/03).

6. As per claims 1, 18 and 49:

Hill discloses "A method for managing security event data collected from a security devices in a distributed computing environment" in (Figure 1) "comprising the steps of:

generating a plurality of alerts with a plurality of security devices at a first location" in (Col 4 lines 30-40);

"providing one or more variables operable for analyzing and filtering security event data, the variables comprising at least one of a location of a security event, a source of security event, a destination address of the security event, a security event type, a priority of a security event, and an identification of a system that detected a security event" in (Col 5 line 39 to Col 6 line 20);

"creating scope criteria by selecting one or more of the variables operable for analyzing and filtering security event data, the security event data comprising the plurality of alerts" in (Col 5 lines 25-45);

"collecting security event data generated by the plurality of security devices located at a first location" in (Col 4 lines 30-40);

"storing the collected security event data at a second location" in (Col 8 lines 12-19);

"analyzing and filtering the collected security event data with the scope criteria to produce result data" in (Col 5 lines 15-20);

“transmitting the result data to one or more clients; and

displaying the result data comprising filtered alerts based on the scope criteria” in

(Col 5 lines 20-45, Col 8 lines 4-11, and Col 8 line 63 to Col 9 line 7).

7. As per claims 2, 21, 35, and 54:

Hill discloses “The method of claims 1, 16, 34, and 49, further comprising storing one or more of the scope criteria, the security event data, and the result data in a database

(Col 8 lines 12-19).

8. As per claim 3, 5, 20, 30 and 36:

Hill discloses “the method of claims 1, 16, and 27, wherein the first location is a distributed computing environment (Figure 1), the second location is a database server (Col 8 lines 12-19), and the third location is an application server (Col 5 lines 15-20) to which the plurality of clients are coupled”.

9. As per claims 4, 14, 19, 38, 47, and 53:

Hill discloses “the method of claims 1, 16, 34, and 49, wherein collecting the security event data comprises generating security event data from a sensor” in (Col 4 lines 30-40); “sending the security event data from the sensor to a collector” in (Col 8 lines 12-19); and “converting the event data to a common format” in (Col 5 lines 37).

Art Unit: 2135

10. As per claims 6 and 39:

Hill discloses “the method of claims 1 and 35, further comprising searching the stored security event data for additional information identifying a security event” in (Col 5 lines 26-45).

11. As per claims 7 and 40:

Hill discloses “the method of claims 1 and 35, further comprising: polling a database server for current stored security event data; analyzing the current stored security event data to produce current result data; and rendering the current result data” in (Col 5 lines 26-45).

12. As per claims 8 and 41:

Hill discloses “The method of claims 1 and 34, further comprising polling for messages containing information about scope criteria, security event data, or result data (Col 5 lines 26-45).

13. As per claims 9 and 42:

Hill discloses “The method of claims 1 and 34, further comprising pushing messages to a client wherein the messages contain information about scope criteria, security event data, or result data (Col 4 lines 30-40, and Col 8 lines 4-11).

14. As per claims 10, 17, 43, and 50:

Hill discloses “The method of claims 1, 16, 34, and 49, wherein the step of rendering result data comprises presenting the result data in a chart format (Figure 7).

Art Unit: 2135

15. As per claims 11, 22, 44, and 55:

Hill discloses "The method of claims 1, 16, and 34, wherein in response to analyzing the collected security event data, an action is executed (Col 7 line 63 to Col 8 line 12).

16. As per claims 13, 24, 46, and 57:

Hill discloses "The method of claims 11, 22, 44, and 55, wherein the action is creating an incident from result data for preparing a response (Col 7 line 63 to Col 8 line 12).

17. As per claims 15, 26-27, 48, and 59:

Hill discloses "A computer-implemented system for managing security event data collected from a plurality of security devices comprising: a plurality of security devices operable for generating security event data comprising a plurality of alerts" in (Col 4 lines 3-40); "an event manager coupled to the security devices, the even manager operable for collecting security event data from the security devices and analyzing the security event data with scope criteria comprising a plurality of definable variables operable for analyzing the security event data" in (Fig 1, Col 8 lines 14-19, and Col 5 lines 7-45); "providing one or more variables operable for analyzing and filtering security event data, the variables comprising at least one of a location of a security event, a source of security event, a destination address of the security event, a security event type, a priority of a security event, and an identification of a system that detected a security event" in (Col 5 line 39 to Col 6 line 20, Col 8 lines 23-35); and "one or more clients coupled to the event manager operable to perform an action in response to receiving analyzed security event data from the event manager and displaying the result

Art Unit: 2135

data comprising filtered alerts based on the scope criteria" in (Col 7 line 64 to Col 8 line 11 and Col 8 line 63 to Col 9 line 7).

18. As per claims 16, and 34:

The rejection basis of claims 1, and 27 is incorporate. Further, Hill discloses applying the scope criteria to the security event data at a third location to produce a result, the result accessible by a plurality of clients coupled to a server" in (Fig 1, Col 8 lines 15-35, and Col 5 lines 45-65).

19. As per claim 25:

Hill discloses "the method of claim 16, further comprising applying additional scope criteria to a plurality of results" in (Col 7 lines 40-63).

20. As per claim 28:

Hill discloses "the system of claim 27, wherein the event manager comprises a database server operable for storing the collected security event data and the analyzed security event data" in (Col 8 lines 12-19, and Col 7 lines 45-65)

21. As per claim 29:

Hill discloses the system of claim 27, wherein the event manager comprises an application server operable for creating an incident from the security event data for preparing a response (Col 8 lines 1-21).



Art Unit: 2135

22. As per claim 31:

Hill discloses the system of Claim 27, wherein multiple clients operable for receiving analyzed security data are coupled to the event manager (Col 8 lines 1-21).

23. As per claim 32:

Hill discloses "The method of Claim 27, wherein the action performed by the client is rendering a chart containing analyzed security event data (Figure 7).

24. As per claim 33:

Hill discloses "The method of Claim 1, further comprising the step of rendering the result data in a manageable format for the plurality of clients (Figure 7).

25. As per claim 37:

Hill discloses "The method of Claim 34, further comprising editing the scope criteria (Col 5 lines 1-6 and Col 5 lines 25-38).

26. As per claims 37, and 51-52:

Hill discloses "The method of Claims 1, and 49, further comprising the step of creating and editing the scope criteria for filtering the security event data (Col 5 lines 1-6, and Col 5 lines 25-38).

***Claim Rejections - 35 USC § 103***

27. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

28. Claims 12, 23, 45, and 56 are rejected under 35 U.S.C. 103(a) as being unpatentable over Hill.

29. As per claims 12, 23, 45, and 56:

Hill discloses "The method of claims 11, 22, and 44. However, Hill does not mention the action is clearing security event data from storage. Nevertheless, it would have been obvious at the time of the invention for one having ordinary skill in the art to realize that the capability of clearing out the data must be exist in the invention of Hill, since it is inevitable to contain unlimited data in any storage devices.


Art Unit: 2135

30. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Linh LD Son whose telephone number is 571-272-3856. The examiner can normally be reached on 9-6 (M-F).

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Vu can be reached on 571-272-3859. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Linh LD Son  
Examiner  
Art Unit 2135

  
HOSUK SONG  
PRIMARY EXAMINER